United States
Department of
Agriculture

Office of
The Chief
Information
Officer

Cyber Security
DM 3500-002
Chapter 6

USDA Vulnerability Scan Procedures

SECURITY PROTECTION
TABLE OF CONTENTS

DEPARTMENTAL MANUAL	NUMBER: 3500-2
SUBJECT: Security Protection	DATE: April 4, 2003
	OPI: OCIO. Cyber Security

CHAPTER 6
GENERAL INFORMATION

1 PURPOSE

This Departmental Manual chapter establishes the policy and procedures for the use of Security Protection for Information Technology (IT) assets within USDA. Security Protection includes the use of Gateways, Firewalls, Intrusion Detection Systems, Public Key Infrastructure (PKI) Technology, IBM/IBM Compatibles Mainframe Security Standards, Identification & Authentication, Vulnerability Scans, and User Logon Identification. Each of these areas will be covered in separate parts of this chapter.

Part 1, Vulnerability Scan Procedures, defines policy and procedures for conducting vulnerability scans in USDA. In addition, this part establishes requirements for an IT inventory, monthly scans of IT equipment for vulnerabilities, reporting, and a requirement for action plans to correct critical vulnerabilities by all USDA agencies and mission areas.

2 CANCELLATION

This Departmental Manual chapter will be in effect until superseded.

3 REFERENCES

The Computer Security Act of 1987;

National Institute of Standards and Technology Special Publication 800-3;

DISTRIBUTION:

Office of Management and Budget Circular A-130, Appendix III;

DR3300-1, Telecommunications & Internet Services and Use.

4 SCOPE

This manual applies to all USDA agencies, programs, teams, organizations, appointees, employees and other activities.

5 ABBREVIATIONS

CIO	- Chief Information Officer
CS	- Cyber Security
DAA	- Designated Accrediting Authority
IP	- Internet Protocol
ISS	- Internet Security Systems
IT	- Information Technology
NIST	- National Institute of Standards and Technology
OCIO	- Office of the Chief Information Officer
OMB	- Office of Management & Budget
USDA	- United States Department of Agriculture

6 DEFINITIONS

a Computer System – This term applies to any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. This includes computers, ancillary equipment, software, firmware, and similar procedures, services, including support services and related resources as defined by regulations

issued by the Administrator for the General Services Administration.

b Designated Accrediting Authority - From a security perspective, all USDA General Support Systems (GSS) and Major Software Applications (MSA) are required to undergo a security certification process and be accredited by a Designated Accrediting Authority (DAA) prior to being placed in operation. The implementation of a formal configuration management process is a requirement for system accreditation. The documentation maintained for configuration management will also provide the necessary evidence to the DAA that the security aspects of each change since the system's last accreditation review have been properly evaluated.

c Internet Protocol (IP) address – A numeric address allocated to identify nodes on a TCP/IP network. These addresses can be statically or dynamically allocated. The current addressing scheme on the Internet is know as IPV4.

d Inventory – The process of making a detailed list of equipment in one's possession.

e Mitigation – The process of moderating in force or intensity; alleviate.

f Network – A group of two or more computer systems linked together. Local-Area networks and Wide-Area Networks are two examples of networks.

g Server – A server is a computer or device on a network that manages network resources. Servers are often dedicated, meaning that they perform no other tasks besides their server tasks.

h Security Vulnerability – A weakness in the software and/or hardware design that allows circumvention of the system security.

CHAPTER 6, PART 1
VULNERABILITY SCAN PROCEDURES

1 BACKGROUND

Global network connectivity is commonplace for information exchange and is crucial for conducting many everyday operations. However, the benefits can be overshadowed by the increase in network vulnerabilities. The number of Information Technology (IT) related incidents that have occurred in the past year, along with the increase and complexity of threats, requires that USDA take their security protection measures seriously. Networks and information technology resources are continually vulnerable to illegal/ malicious activity or exploitation by internal and external sources.

Vulnerability Scan Procedures are a critical component of the Overall Security Protection Plan within the Department. Regular IT inventories and vulnerability scans have proven to be an effective tool in combating IT incidents and exploits of USDA information assets. The purpose of this document is to establish the policy and procedures for the inventory and vulnerability scans of all USDA managed networks, systems, and servers.

2 POLICY

All USDA agencies and mission areas will establish and implement the following procedures for accomplishing vulnerability scanning of all networks, systems, and servers for which they have responsibility. Each agency/mission area will report to CS all Critical Vulnerabilities (High and Medium) found as a result of the scan. Internet Security Systems (ISS) scanner software will be used to scan networks, systems and servers that will be obtained from the Department-wide Contract Vehicle established for this purpose. The ISS Software already classifies the vulnerabilities into high, medium and lows with default values from the vendor. Vulnerability Scans are to be performed on a <u>monthly</u> basis for all networks, systems, and servers by duly authorized users in accordance with established procedures. Cyber Security also requires that Discovery Scans be performed monthly to ensure that there are no “unauthorized

devices" on agency networks. Agencies will run scans inside USDA using USDA owned IP addresses, unless they have an approved waiver to deviate from this policy. Other types of workstation scans are an option of the ISS scanner software but not required by this policy. Physical or electronic inventories can be done of network, systems and servers. However, electronic inventories are preferable. Each agency will designate authorized personnel to conduct software scans. All authorized users will be trained in the use of the scanner software prior to conducting any internal or external scans and will notify the CS before running scans. The National Intrusion Detection System (IDS) managed by CS detects all scans whether they originate externally or internally. Agencies/staff offices will identify the range of Internet Protocol (IP) addresses to be scanned and the IP address of the platform being used to launch the scan. Agencies and staff offices will not attempt to scan networks, systems, or servers for which they are not responsible.

All new Information Technology (IT) systems will be scanned by authorized users prior to deployment into a production environment. Agencies and staff offices will produce and retain inventory and vulnerability scan reports for all scans conducted for a minimum of six months. Vulnerabilities will be reported on the Host Vulnerability Summary Report (Sorted by IP Address) in the ISS Program. These reports can be archived on CDs to reduce space concerns. A summary of the vulnerabilities identified will be provided to the agency IT Managers/Chief Information Officer for review to ensure that corrective action plans are developed within 60 days and implemented for critical vulnerabilities identified. Critical vulnerabilities are those that have the potential to disrupt the operation of networks and servers used to transport USDA data. A copy of the Summary of the Security Vulnerabilities (with associated Action plans) identified by each agency/mission area will be provided to the Associate CIO for Cyber Security. Action plans will be updated monthly with status until necessary security mitigations are in place or the risk is officially accepted by the DAA or agency CIO.

Waiver Requirements. A written waiver request, with a persuasive and cogent justification, will be prepared for all actions not taken to mitigate critical vulnerabilities. Agencies do not prepare waivers for "false positives". Waiver requests will be sent to the Associate CIO for Information Resources Management (IRM) to be forwarded to CS for review and further action. In general, security policy dictates

that agencies/staff offices make every reasonable effort to correct critical vulnerabilities to USDA networks, systems and servers.

3 RESPONSIBILITIES

a The Associate Chief Information Officer for Cyber Security will:

(1) Provide customer support to agencies and staff offices in obtaining Internet Security Scanners, Scanning Software and Keys from the USDA Enterprise License Contract.

(2) Assist agencies/staff offices in obtaining training on the use of scanning equipment on their networks, systems, and servers;

(3) Provide technical guidance in scanner use to agencies and staff offices, as required, after training of authorized users has taken place;

(4) Conduct oversight reviews of agencies and staff offices to review vulnerability reports and corrective actions taken to ensure that networks, systems, and servers are protected in accordance with this policy; CS also reserves the right to review Discovery Scans;

(5) Establish, maintain, and monitor a database of agency/staff office critical vulnerabilities and action plans identified in the Scan Summary Report; establish and maintain copies of agency/mission area IP addresses; and

(6) Review all waivers requesting exceptions to this policy in a timely manner and coordinate the response to the agency with the Associate CIO for IRM.

b The Associate CIO for Information Resources Management (IRM) will:

(1) Support the policy and procedures contained in this chapter to ensure that appropriate security protection is provided to all USDA managed networks, systems and servers; and

(2) Receive, review and coordinate a response with the Associate CIO for Cyber Security to any waiver requests for exceptions to this policy.

c Agency Management and Information Technology Officials or Chief Information Officer will:

(1) Implement and enforce this policy and procedures within all internal agency/staff office activities who are responsible for network, systems, workstations, and servers;

(2) Ensure that all agency/staff offices order and use the Internet Security Scanner software and keys in conducting internal and external scans on a monthly basis and that inventories of networks, systems, servers, software and Internet Protocol (IP) addresses are maintained;

(3) Designate and notify CS of personnel authorized to conduct agency/staff office scans; ensure that these personnel are trained; notify Cyber security prior to conducting any scans;

(4) Review Scan Report Summary information on a monthly basis to ensure that critical vulnerabilities identified are corrected in a timely manner;

(5) Provide a monthly report of inventories and a summary critical vulnerabilities (high & medium) uncovered using the scan tools to the Associate CIO for Cyber Security with an Action Plan (including timeframes) for mitigating these vulnerabilities within 60 days; false positives are not be to be reported;

(6) Vulnerability Reports will be reported on ISS Report Format, Host Vulnerability Summary Report, Sorted by IP Address on a monthly basis. These reports will be saved in Rich Text Format (RTF) and sent to CS electronically;

(7) Submit a waiver package, including a strong justification, for all critical vulnerabilities when corrective actions are not taken and forward to the Associate CIO for IRM for review and action; and

(8) Take necessary action to archive IP addresses, IT equipment inventory and vulnerability reports for at least 6 months.

d The agency Information Systems Security Program Managers (ISSPM), Systems/Network Administrators or Authorized Users will:

(1) Assist in performing monthly inventories and vulnerability and discovery scans of all agency/staff office managed networks, systems, workstations, and servers as the authorized user;

(2) Assist in performing vulnerability scans of all new systems, network, or servers prior to production deployment and to existing systems after major changes are made;

(3) Assist in producing/updating inventory and vulnerability reports for all agency/staff office managed networks, servers, software and IP addresses on a monthly basis;

(4) Document in a Summary Report all vulnerabilities noting those which are critical and identify corrective actions with recommended timeframes;

(5) Forward the Summary Report to the Agency IT or Chief Information Officer for review and further action;

(6) Document the status of actions taken by all Authorized Users to mitigate vulnerabilities identified or prepare a written waiver package with a strong justification to agency/staff office IT Manager/CIO for actions not taken; and

(7) Ensure that a current IP Address Report, Inventory Report and Summary of Vulnerabilities (with Action

Plans) are provided to Cyber Security on a monthly basis.

e Agency System/Network Administrators (not Authorized Users) will:

(1) Deploy new systems into production or operational status only after vulnerabilities are resolved through security mitigations or accreditation by the Designated Accrediting Authority (DAA)/agency CIO;

(2) Apply patches or fixed to agency/staff office managed networks, systems, and servers in a timely manner as appropriate;

(3) Keep a written record of all patches and fixes applied to agency/staff office managed networks and servers, including the version and date; Cyber Security reserves the right to verify all written records of system/network/server patches;

(4) Collaborate with the ISSPM/Authorized Users in ensuring that IP Address updates, inventory of IT equipment and vulnerability scans are conducted/updated on a monthly basis; and

(5) Assist the ISSPM/Authorized Users in ensuring that mitigation actions are taken promptly for all critical vulnerabilities or that a persuasive and cogent written justification is provided to agency/staff office IT Manager/CIO for actions not taken.

-END-

Appendix A
Internet Scanner User's Guide

August 13, 2000

Overview of Internet Scanner

Introduction

Internet Scanner is a vulnerability assessment product that analyzes the security of devices on an enterprise-wide network, checking for vulnerabilities on routers, Web servers, Unix servers, and Windows NT servers, desktop systems, and firewalls.

Internet Scanner can be used on all TCP/IP-based networks, networks connected to the Internet, and on stand-alone networks and machines.

Benefits of Internet Scanner

There are many benefits that Internet Scanner provides. Some include:

- Internet Scanner performs the widest variety of vulnerability detection, ranging from gathering information to finding vulnerabilities.
- Internet Scanner finds vulnerabilities much as an intruder would, by examining network devices, services, and interrelationships.
- Internet Scanner provides detailed information about each vulnerability, such as the vulnerable host, description, and corrective actions.
- Internet Scanner also provides different levels of reporting for different audiences, such as illustrated management reports. Other reports include the Summary and Detailed Host Vulnerability reports for administrators.

Components of Internet Scanner

There are four major components that are installed as part of the Internet Scanner application. They are:

Component	Description
Scan Engine	Executes network tests, probing to identify devices and risks
User Interface • GUI • Console • Command Line	Configures and executes risk assessments. • If assessments are performed interactively, risk information appears on the user interface as it is collected to allow online analysis of detected vulnerabilities • If assessments are performed non-interactively (scheduled), command-line interfaces allow sophisticated control.
Reporting Module	Generates hard and soft copy reports for distribution to appropriate parties. • Technical information for Systems Administrators • Summaries for Security Managers
X-Force Security Knowledge Database	Internet Scanner offers more than 1000 checks based on the research provided by X-Force, Internet Security Systems research and development organization. This knowledge resides in a database that provides information useful to planners and practitioners, such as description, risk level, and possible mitigating actions.

Installing Internet Scanner

Requirements for Installation

These items are required when installing Internet Scanner.

- Internet Security Systems Internet Scanner CD or install file. Check with your Information Systems Security Program Manager (ISSPM) or security officer on how to obtain the software.
- Key file. A key file is supplied by Internet Security Systems that enables features in Internet Scanner. Without the key, Internet Scanner runs as an evaluation copy and provides only intranet tests on the local computer.
- Windows NT or Windows 2000 installation CD. Internet Scanner may request some files from the CD to enable specific features or tests.

System Requirements for Internet Scanner

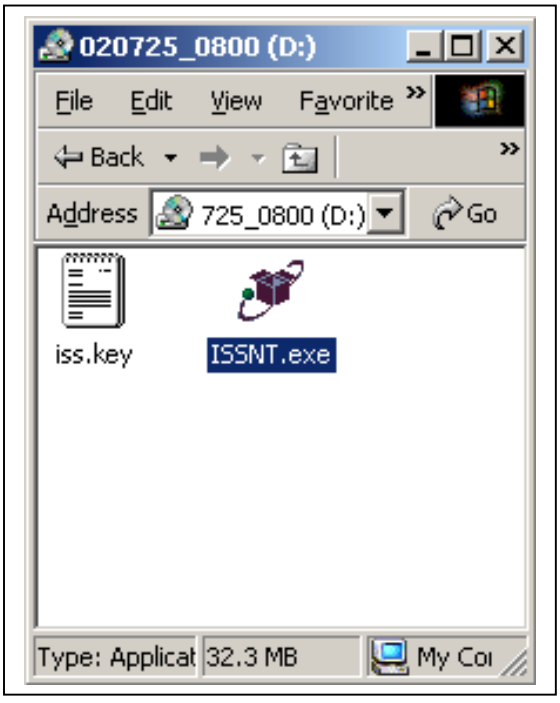
To run Internet Scanner, it is recommended that you use a dedicated system. A dedicated system maximizes performance and protects the system and the data unauthorized access.

Internet Scanner runs on Windows NT 4.0 Workstation or Windows 2000 Professional. All the Internet Scanner components are installed on the same computer system. Internet Security Systems, Inc. does not support Internet Scanner running on the Windows NT 4.0 or Windows 2000 server, although it has been successfully installed and used on servers in USDA.

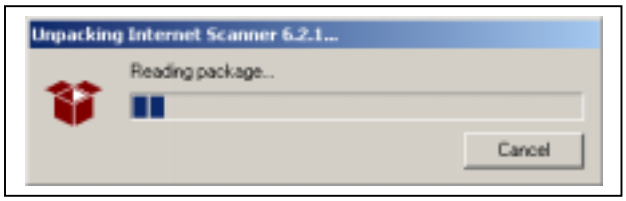
Item	Requirement
Processor	300 MHz Pentium recommended.
Operating System	Windows NT 4.0 Workstation with Service Pack 6, Windows 2000 Professional with Service Pack 2. (Internet Scanner is not supported on Windows NT 4.0 or Windows 2000 server, although it has been successfully installed and used on these systems).
Other software	Microsoft Internet Explorer 5.5 SP2 or later required to run HTML Help. Adobe Acrobat Reader 4.x or later is required to view the PDF files in the Manuals folder.
Memory	For regular scans: 80 MB For large scans: 128 MB (256 MB recommended).
Hard disk	180 MB for installation from the downloaded file or 60 MB for installation from the CD. Drives should be formatted as NTFS.
User privileges	Local or domain administrator.

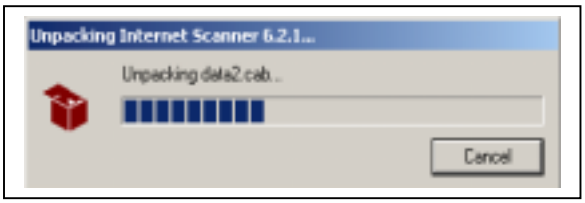
Steps for Installation of Software

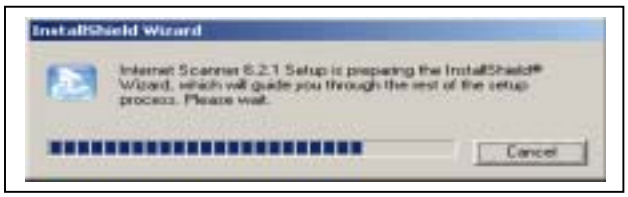
Step 1: From the CD, Shared Drive or your hard drive, **double-click** on the ISSNT.exe icon to launch program.



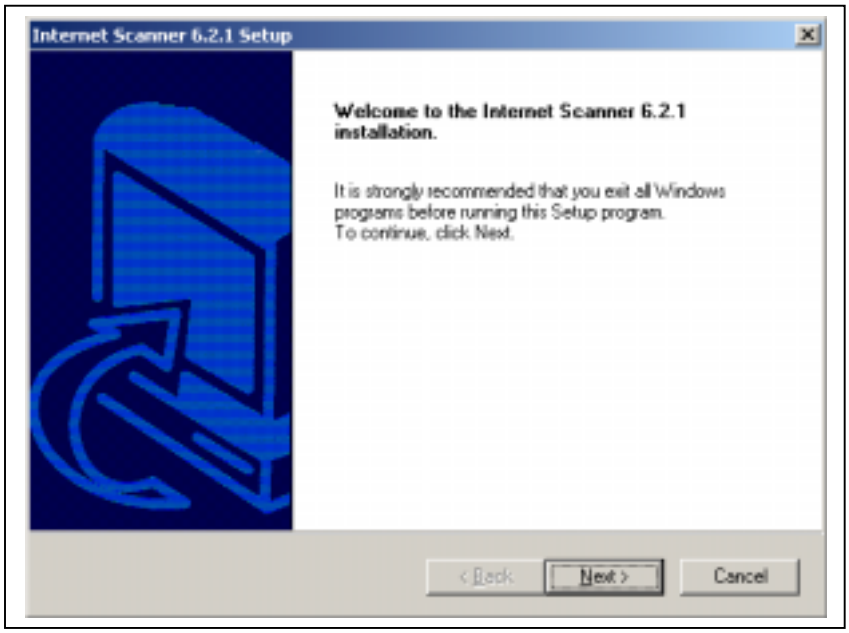
Internet Scanner will start the installation, and you will see the following 3 screens:



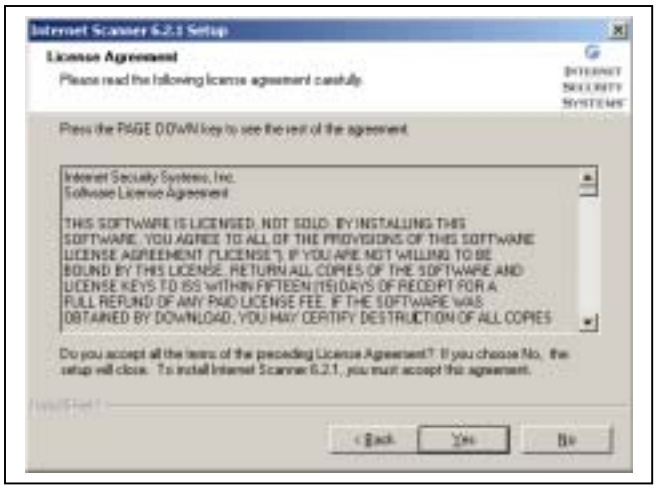




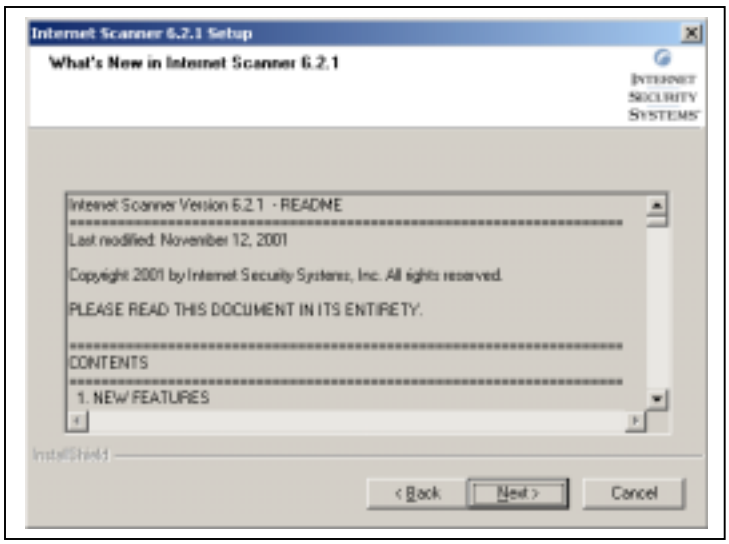
Step 2:
After closing all programs, click **Next** to start the installation process.



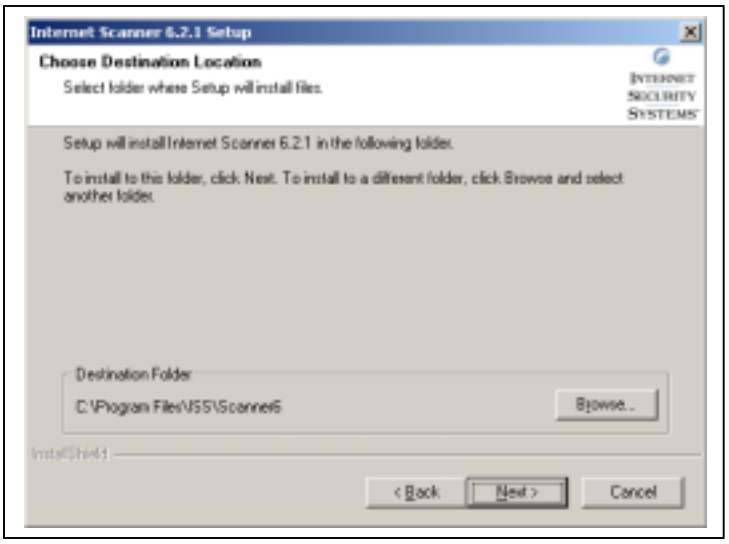
Step 3:
Click **Yes** to accept the license agreement.



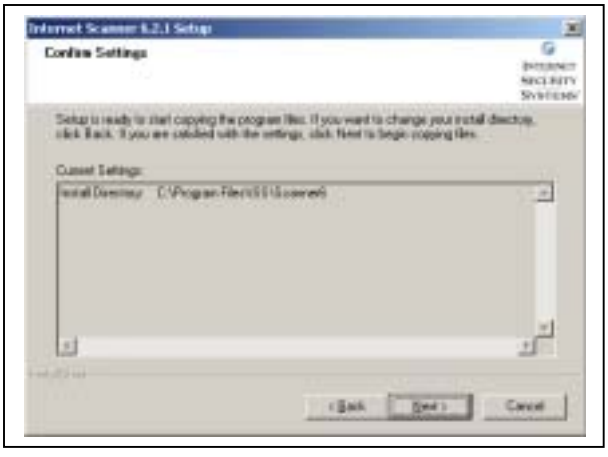
Step 4:
After viewing the readme text, click **Next** to continue



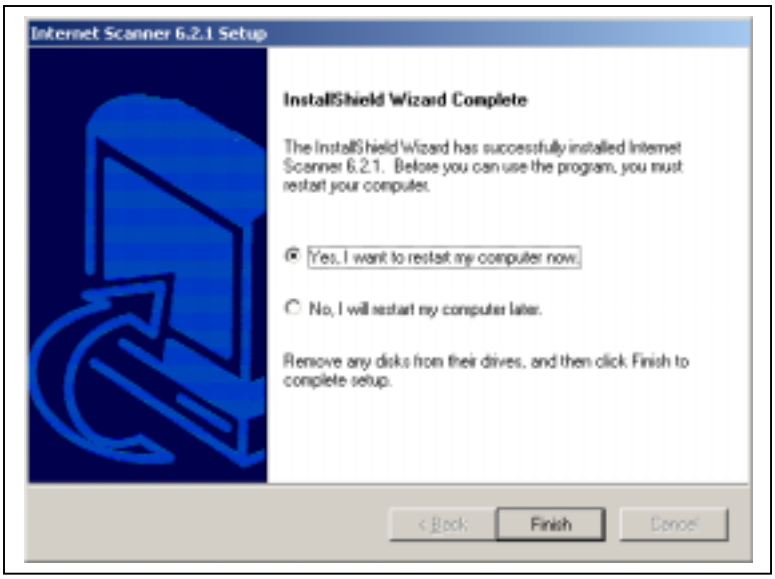
Step 5:
Verify the installation drive and destination, and click **Next.** (Default is c:\program files\iss\scanner6)



Step 6:
Confirm settings and click **Next.** Internet Scanner will start copying program files to your computer.



Step 7:
Select "Yes, I want to restart my computer now", and click **Finish** to complete the installation. Computer will reboot.



X-Press Updates

Introduction

X-Press Updates are packages of new security checks for Internet Scanner. They updates work much like virus updates for antivirus software. These updates are usually released on a monthly basis. Internet Scanner has an X-Press Update Installer program that checks for downloads and installs X-Press Updates. The installer can be run automatically as often as you wish.

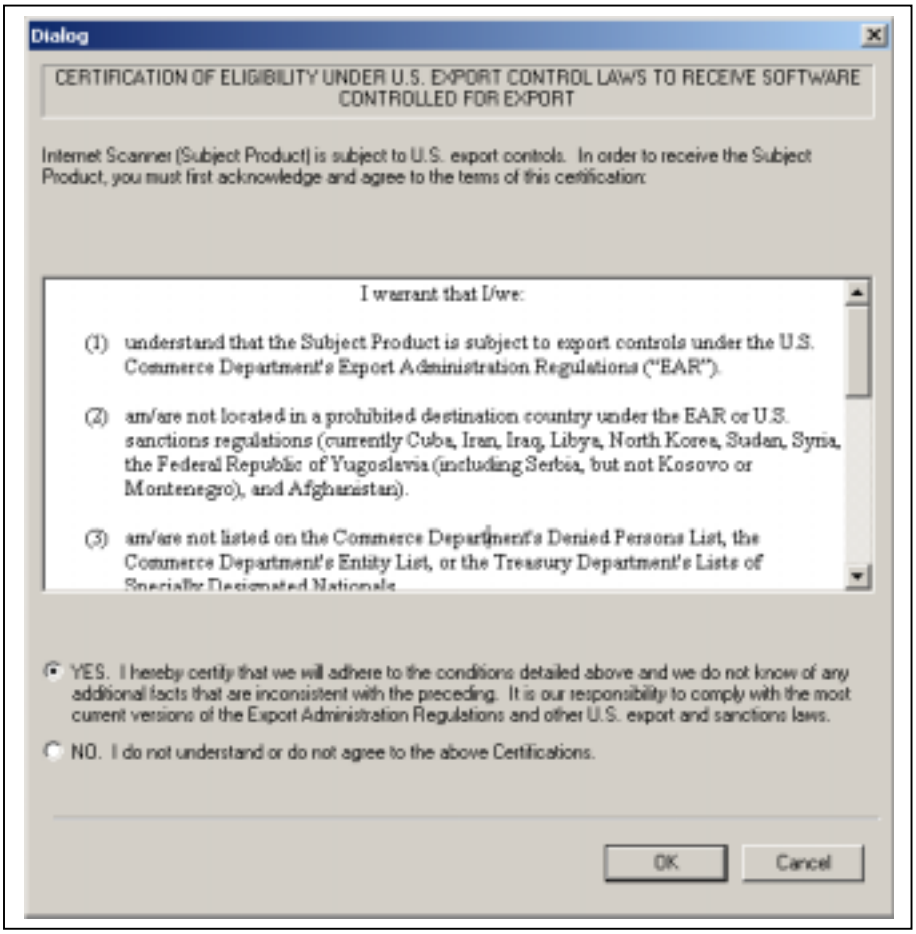
Running X-Press Updates

X-Press Updates automatically update your system with the latest checks and latest product updates available for Internet Scanner. To install new X-Press Updates not currently on your system, follow these steps:

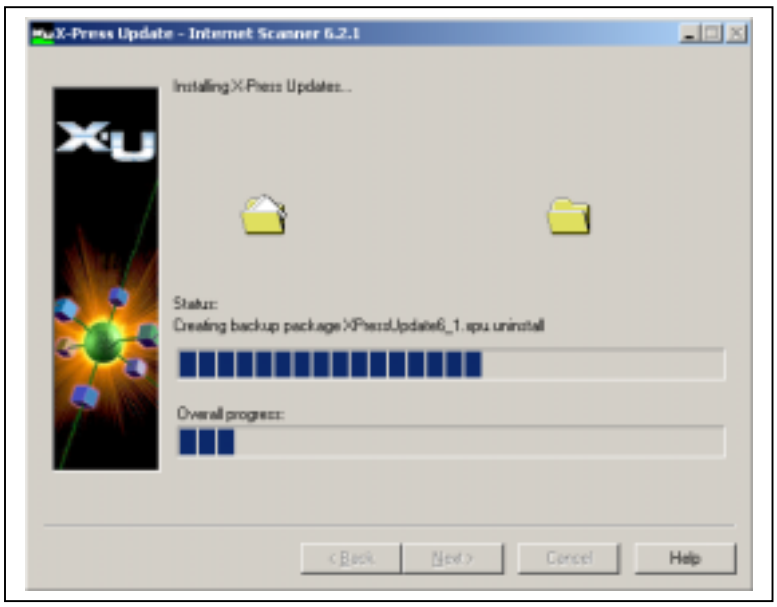
Step 1:
Click Start|Program|ISS|Internet Scanner|X-Press Update Install.

Step 2:
The Select Location window is displayed. **Select** Web Server option, and **Check** Install all new X-Press Updates found. Click **Next** to continue.

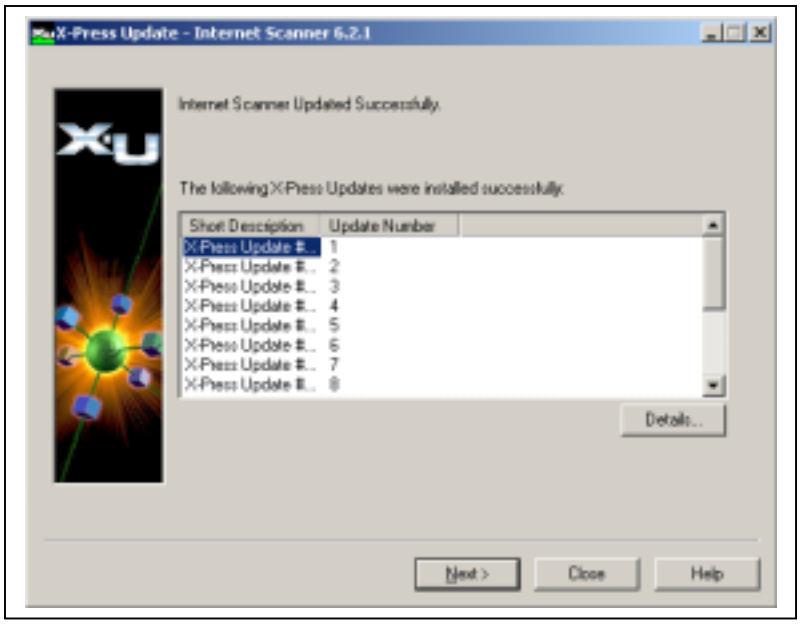
Step 3:
Select **Yes** to agree to the Export Law Agreeement, and then **Click** OK.



X-Press Updates will show the following status screen when updating.



Step 4:
X-Press Update will show the following screen, when it has successfully completed.
Click Close to exit out the program.



Using Internet Scanner

Software License and Key

An Internet Security Systems Software license key is necessary for Internet Scanner and Database Scanner to function properly. Without the iss.key file, the scanners cannot analyze activity across your network and on your computer system. Before you can use Internet Scanner, you must obtain and install your license key. Your Security Officer or ISSPM will most likely email you your license key as a Key File email attachment.

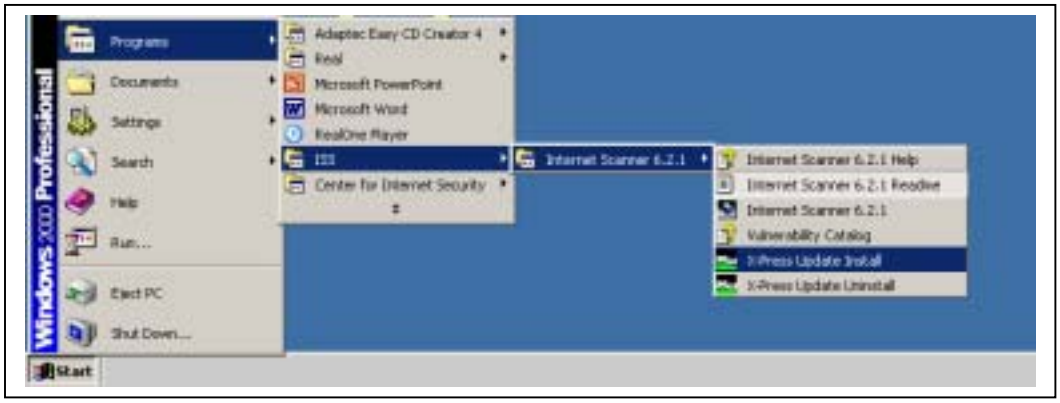
What is a Key File? A key file defines your licensing for Internet Scanner. It contains information such as the products licensed, creation date, maintenance expiration date, and license expiration date. It also lists your valid IP range that you can scan on your network.

Instructions for Installing the License

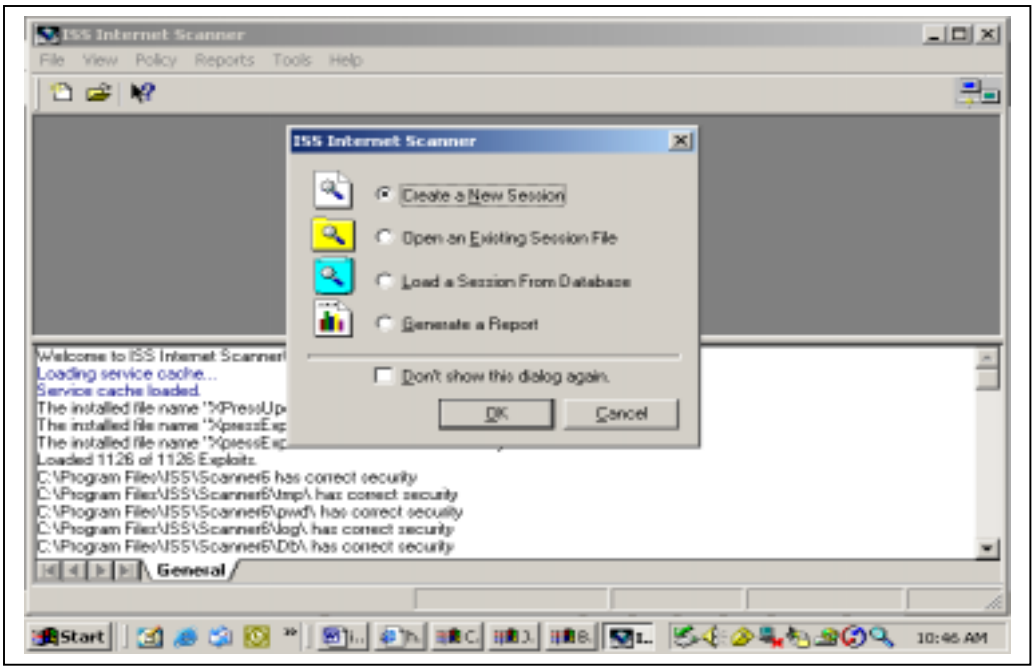
If you receive your Key File license through email, save the entire message (do not copy and paste) using "iss.key" as the filename. Be sure to type the filename in double quotes, especially if using a Windows system, in order to avoid having your system apply some other extension to the file name. save this file in c:\program files\iss\scanner6 directory.

Running Internet Scanner

Step 1: To start Internet Scanner, **Click** Start|Porgrams|ISS|Internet Scanner 6.2.1|Internet Scanner. This will launch the Internet Scanner software.

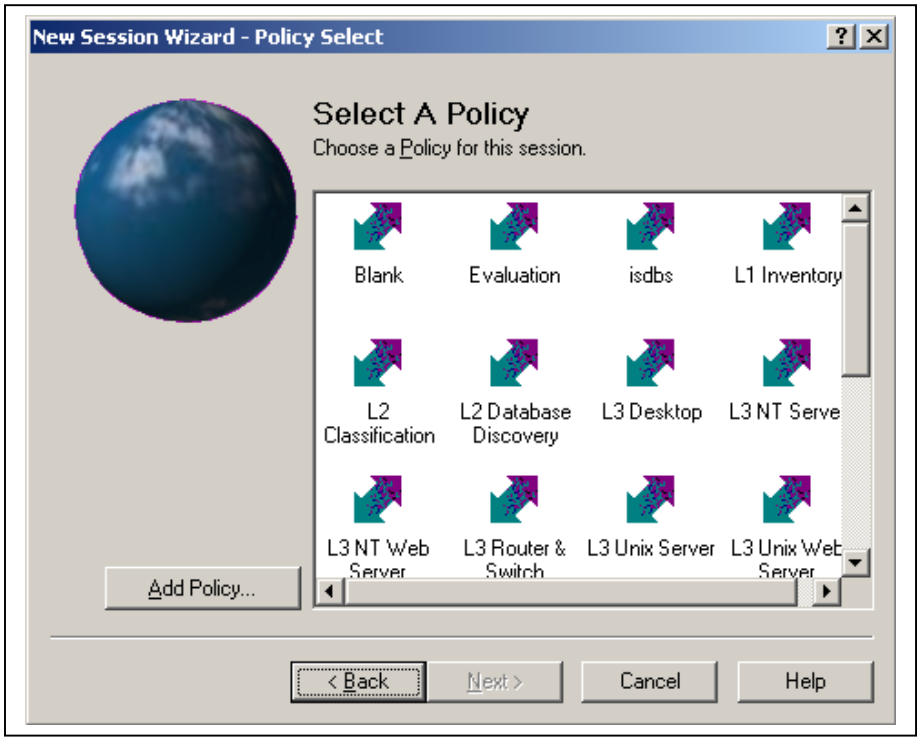


Step 2: **Select** Create a New Session and **Click** OK.

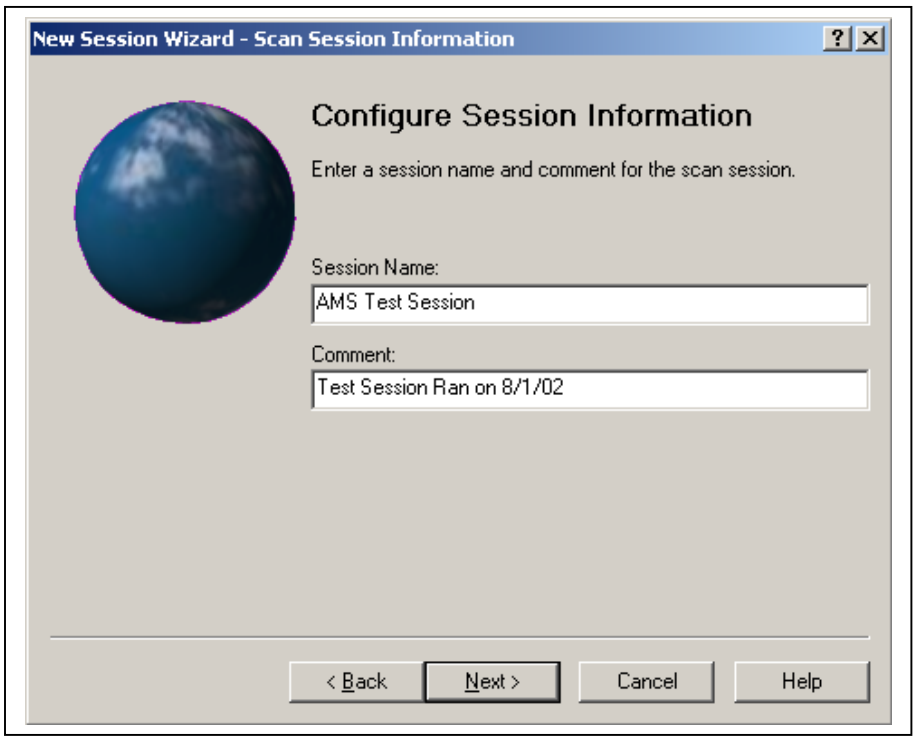


Step 3: **Select** a key that you wish to use for this session and **Click** Next.

Step 4: **Select** the policy that you wish to use, and **Click** Next. For a description of policies, please see "Identifying Security Levels in Internet Scanner" in the next session.



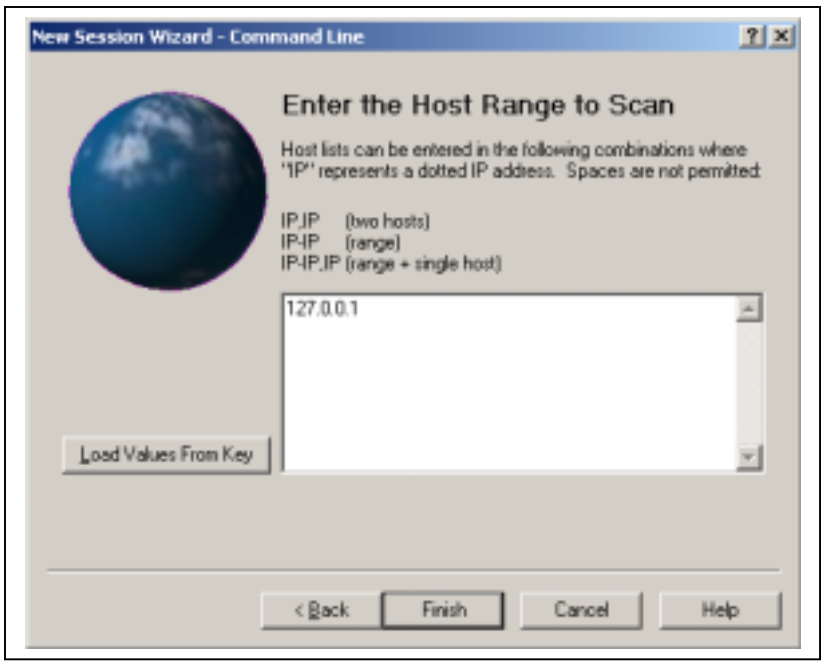
Step 5: **Type** a session name and comment for the scan session and **Click** Next. This will be used to identify the sessions in the Internet Scanner database.



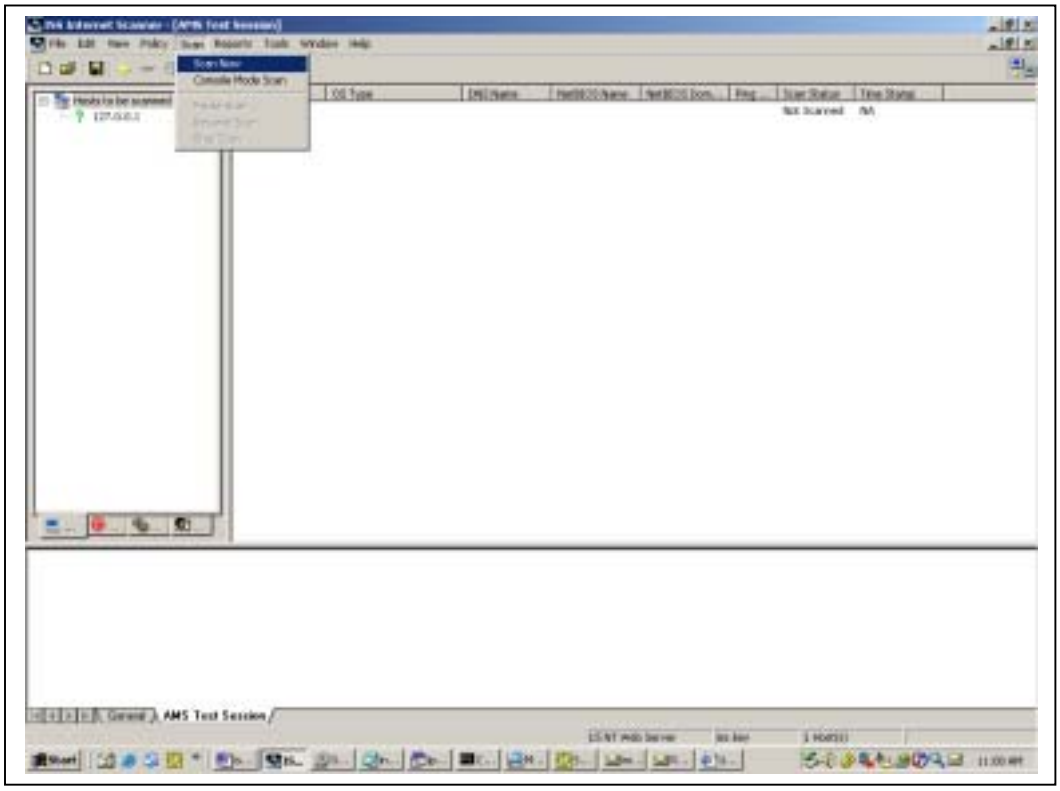
Step 6: This screen chooses how the scanner determines which hosts to scan. **Select** Command Line Facility to manually choose your IP addresses, and **Click** Next.

Step 7: You will get a warning banner indicating that this can cause unnecessary broadcast traffic on the network. **Click** Yes to continue.

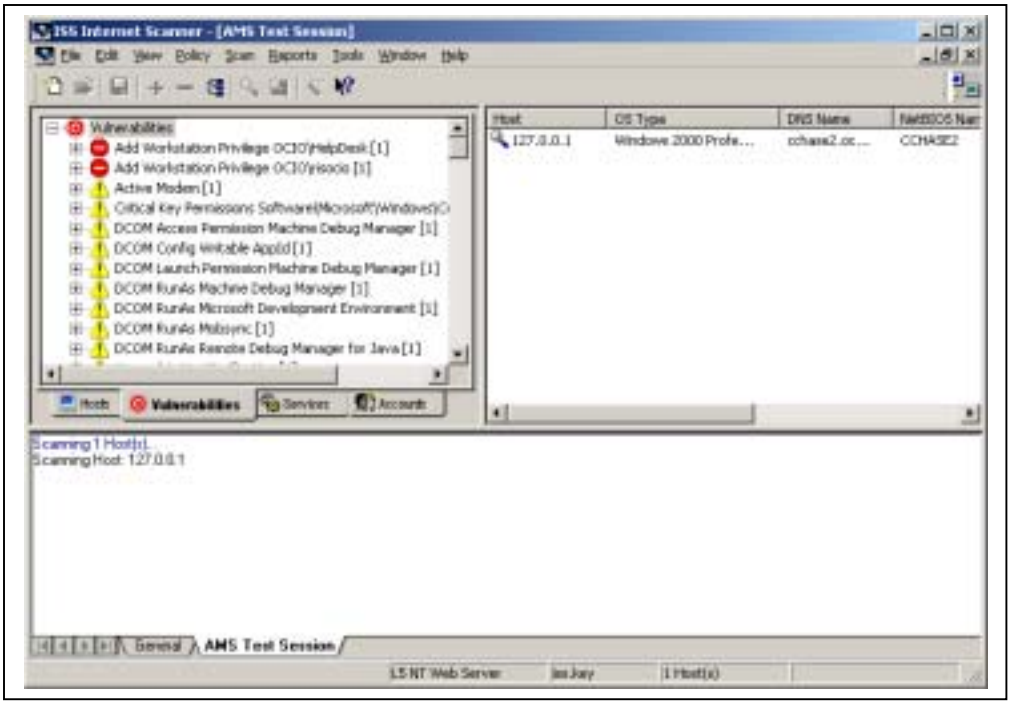
Step 8: **Type** in the host range you wish to scan. When complete, **Click** Finish.



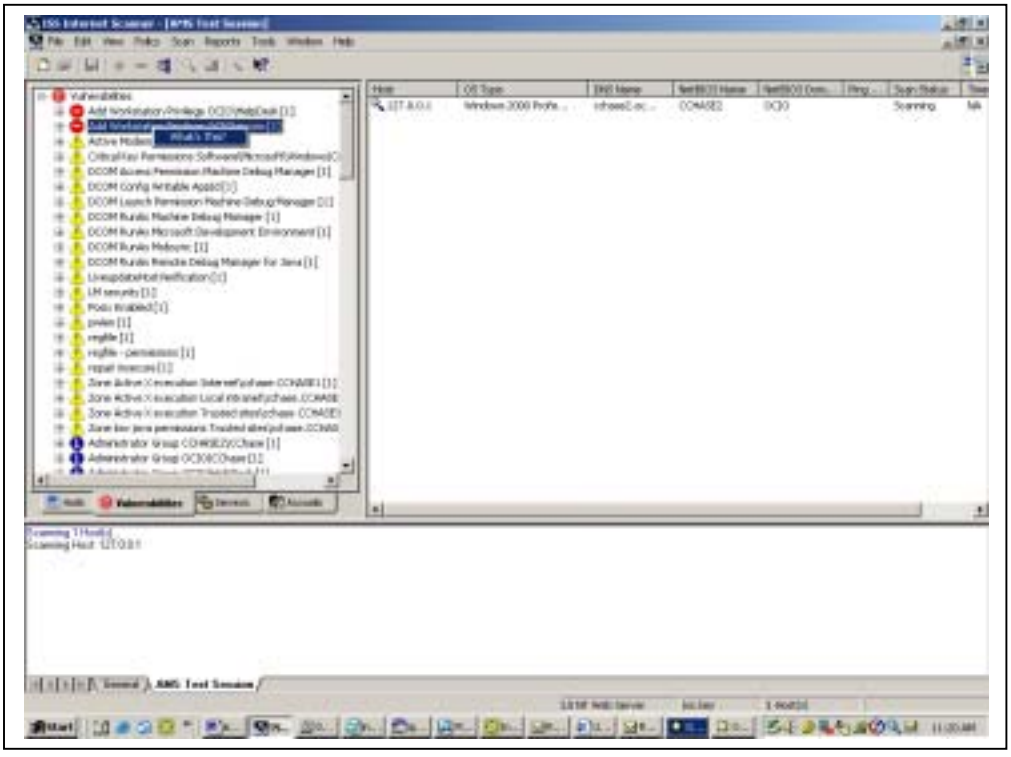
Step 9: Internet Scanner will show the main scanner window. **Click** Scan|Scan Now to start the scan.



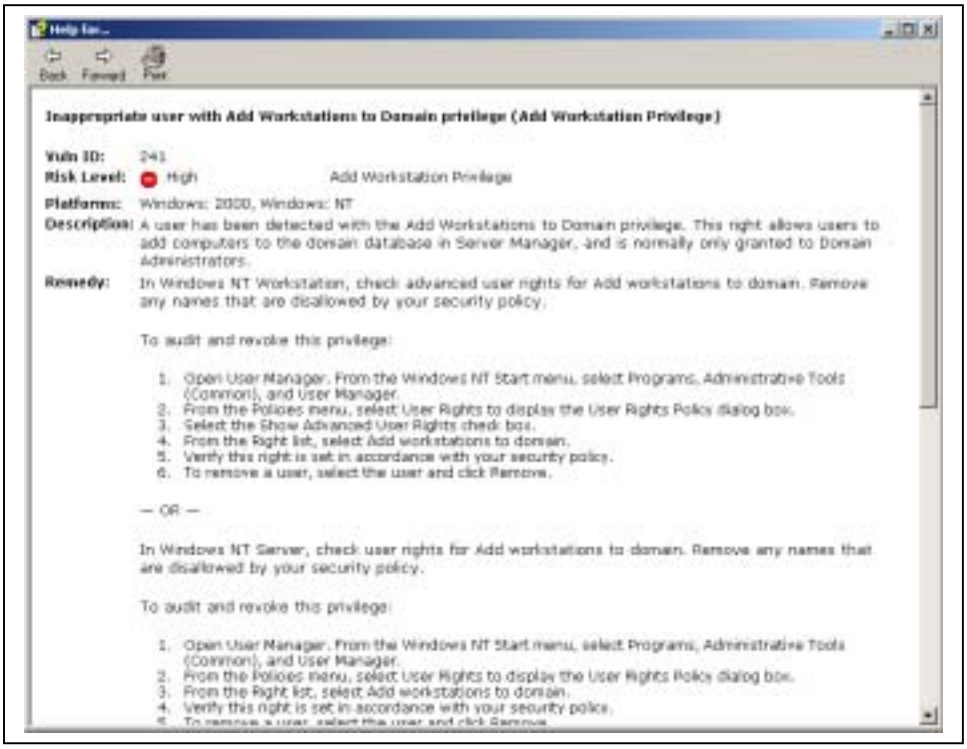
Step 10 (Optional): To view found vulnerabilities while scanning, **Click** on the bullseye vulnerability tab on the lower left frame.



Step 11 (Optional): To view details on the vulnerability, **Right Click** on the item and **Click** "What's This?"



Step 12 (Optional): The help window will appear with the details of your vulnerability.



Step 13: Once scanning has finished successfully, the results will be stored in Internet Scanner's database for retrieval at anytime.

*****Note: For the most thorough scan of your Windows NT and Windows 2000 machines, it is important that you log on the scanning workstation with an account that has administrator rights to both machines. Internet Scanner will use the login credentials of the Internet Scanner machine to probe for vulnerabilities on the machine that you are scanning.**

Identifying Security Levels of Internet Scanner

Internet Scanner offers five levels of security that provide structured and logical approach to managing risk. These groups of security tests are applied to the systems. The higher levels are designed for business-critical systems; the lower risk levels are designed for less important systems. By applying these levels, you ensure that security efforts remain focused on the most important components of the IT infrastructure.

Security levels are types of checks that you apply to particular systems according to the amount of security needed. Level 5 is the most complex of the levels.

The following table lists each level and its description:

Level	**Description**
Level 1	Identifies operating systems of the machines on the network
Level 2	Identifies the services running on machines on the network, such as web servers
Level 3	Checks for compromises by unskilled attackers, or for signs that a system is already compromised.
Level 4	Checks for compromises by automated attack tools, or by moderately skilled attackers
Level 5	Checks for compromises by highly skilled attackers, or for signs that a system is not configured properly.

Internet Scanning Reporting

About Reporting

Reports provide you the ability to view the results of the scan sessions. You can use reports to distribute information to people in your organization that can help correct the vulnerabilities**.**

Report Categories

The reports are grouped into four categories to provide different levels of summary and detailed information. They are:

- **Executive** – provide summary information for speedy assessment of top-level security issues.

- **Line Management** – used for resource planning. Line management reports mainly show details of network scans

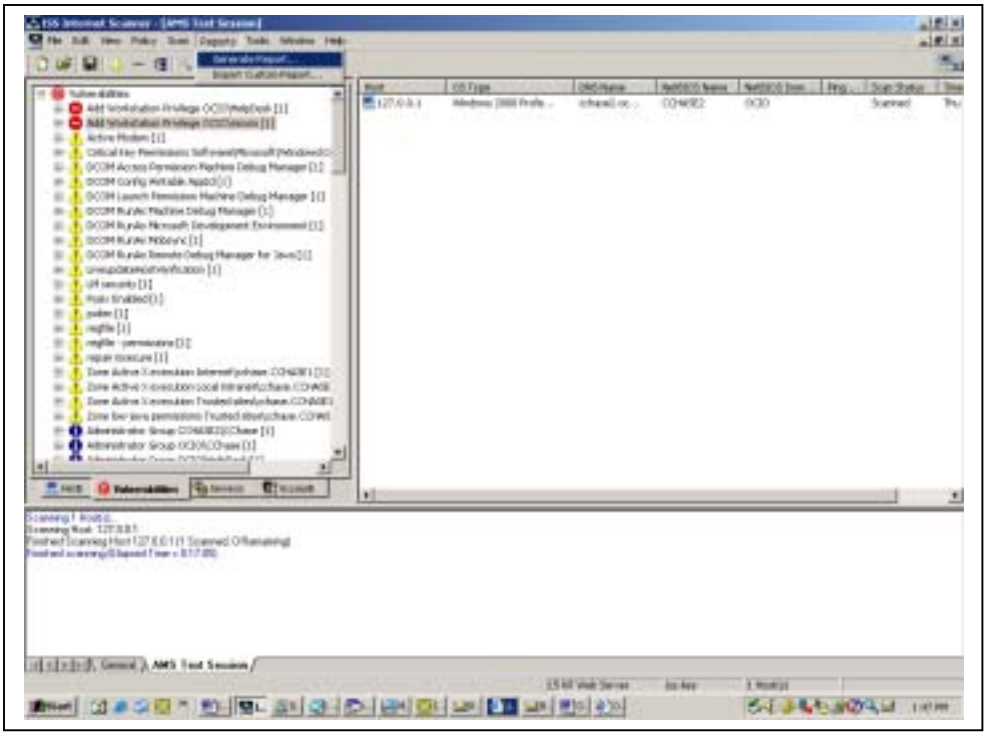
- **Technician** – provides the most detailed information on the status of your network. The descriptions are the same as the Line Management report. This information includes how to fix or patch vulnerabilities detected by Internet Scanner.

- **User Imported** – custom reports based on your own specification.

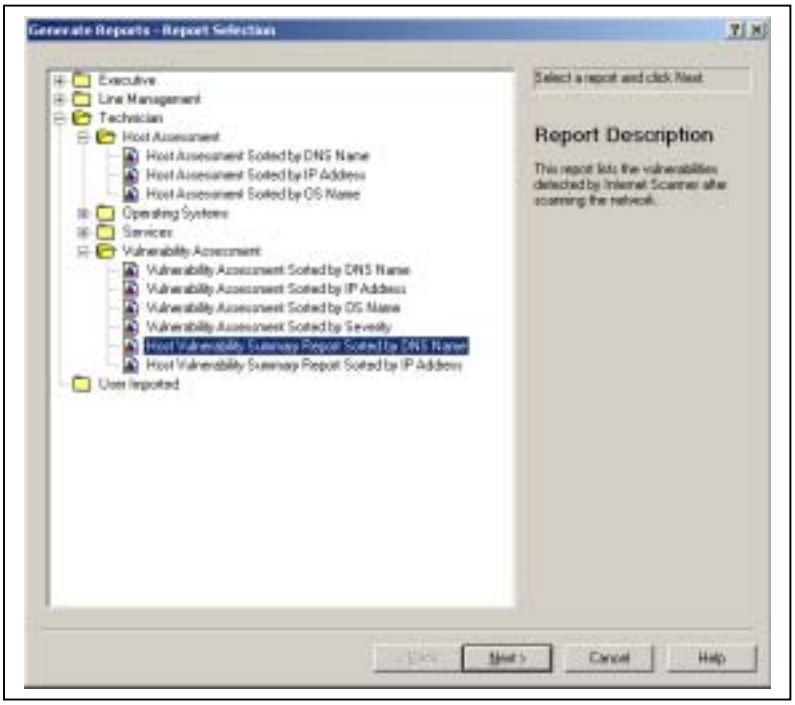
Generating a Report

Step 1: If Internet Scanner is not running, **Click** Start|Programs|ISS|Internet Scanner 6.2.1|Internet Scanner 6.2.1. If Session wizard appears, **Click** cancel.

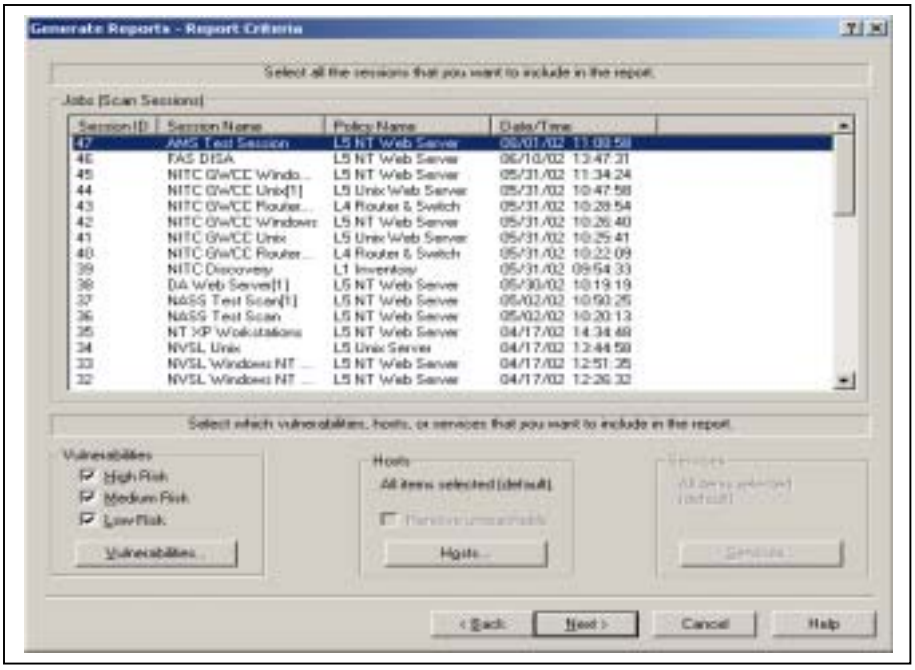
Step 2: Click on Reports|Generate Report



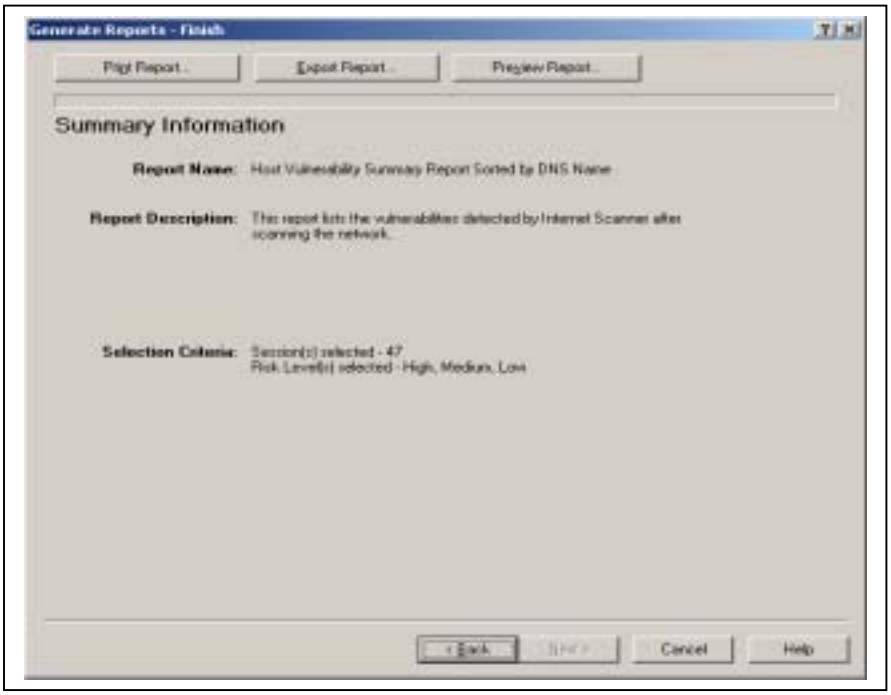
Step 3: From Report Selection, **Select** the type of report that you wish to run. For a description of Technican Reports, see the next session. **Click** Next.



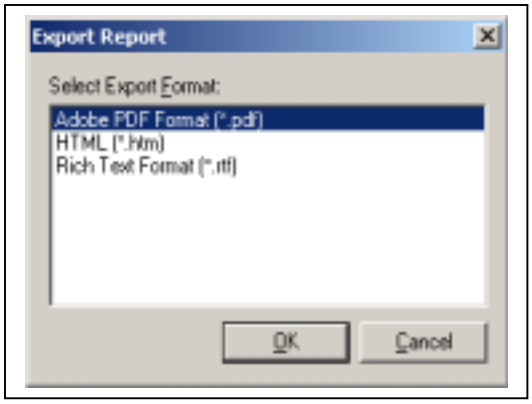
Step 4: Select the session and vulnerabilities that you want to include in this report. **Click** Next.



Step 5: Select Print Report, Export Report or Preview Report to get desired results, for this purpose, we will select Export Report.



Step 6: Select format, and then **OK**. The Select Export File window will appear. **Select** a name and then **Save** to save the report.



Technican Vulnerability Assessment Reports

For Systems Administrators, the most important reports are the Technician Vulnerability Assessment Reports, as they give the most detailed information about vulnerabilities that were found on a particular system. All of the reports in this section gives the same vulnerability details and summaries with the exception of:

Vulnerability Assessment Sorted by DNS Name – This report lists the vulnerabilities detected by Internet Scanner sorted by DNS name as well as the details of account vulnerabilities found in Windows NT environments.

Scheduling Internet Scanner

To run Internet Scanner at specific times during the day, you can use the Windows NT at command from the command line. The at command schedules commands and programs to run on a computer at a specified time and date. The Schedule service must be running to use the at command.

Note: The only method to schedule a scan is from the command line.

You can set up the scheduler to run specific sessions, host files, and reports.

You use the syntax example as shown in the following examples:

At [24 Time]/interactive/every: [Day interval}
"C:\Program Files"\Iss\Scanner6\iss_winnt.exe –s"
"C:\Program Files\iss\Scanner6\<sessionname>.session"

Parameter	Definition
\\computername	Specifies a remote computer. If this parameter is omitted, the commands are scheduled on the local computer
id	Identification number assigned to a scheduled command
/delete	Cancels a scheduled command. If the ID is omitted, all of the scheduled commands on the computer are canceled.
/yes	Forces a yes answer to all queries from the system when deleting scheduled events.
time	Specifies the time when the command is to run. Time is expressed as hours:minutes in the 24-hour notation (00:00 [midnight] through 23:59)
/interactive	Allows the job to interact with the desktop of the user who is logged on a time the job runs.
/every:date[….]	Runs the command on every specified day(s) of the week or month. For example, every Thursday, or every third day of the month. Specify the date as one or more days of the week, such as M, T, W, Th, F, S, Su. Specify one or more days of the month by using the numbers 1 through 31. Separate multiple date entries with commas. If the date is omitted, the current day of the month is used.
/next:date[,…]	Runs the specified command on the next occurrence of the day (for example next Thursday)
"command"	The Windows NT command, program (such as .exe or .com file) or batch program (such as .bat or cmd file) to be run. When the command requires a path as an argument, use the absolute path (the entire pathname beginning with the drive letter). If the command is on a remote computer, specify the server and sharename, rather than a remote drive letter. You may use quotation marks around the command when using either the command line or in a batch file. If the command line includes switches that are used by both the command and at, you must enclose the command in quotation marks. If the command is not an executible (.exe) file, you must precede the command with cmd/c. For example, cmd/cdir>c:\test.out

For Example, if you wanted to run Internet Scanner at 6 p.m. every five days, you can type the following syntax:

At 18:00/interactive/every: 5,10,15,20,25,30 c:\progra~1\iss\scanner6\iss_winnt.exe –s c:\progra~1\iss\scanner6\<session name>.session

Deleting Database Sessions

The session delete tool is a utility that allows a user to delete sessions from the Internet Scanner Access Database.

The tool uses the jobID from the Internet Scanner Access Database to reference the session to delete. A list of available jobids can be displayed by using the list flag.

Usage:
sessiondelete <jobID>
sessiondelete list

Step 1: At the command prompt, **Change** to the c:\program files\iss\scanner6\tools directory.

```
C:\Program Files\ISS\Scanner6\Tools>cd\

C:\>cd program files

C:\Program Files>cd iss

C:\Program Files\ISS>cd scanner6

C:\Program Files\ISS\Scanner6>cd tools

C:\Program Files\ISS\Scanner6\Tools>
```

Step 2: Once at the directory, **Type** "sessiondelete <jobID>, where the job id is the number associated with the job. For a list of jobs, **Type** "sessiondelete list".

```
C:\Program Files\ISS\Scanner6\Tools>sessiondelete 1
Scan session data for job 1 deleted
C:\Program files\ISS\Scanner6\Tools>
```